Völker- vs. Wehrverfassungsrecht – Neue Grenzen des Parlamentsvorbehalts beim Einsatz der Bundeswehr im Cyber-Raum?

Gastautor 2016-06-30T07:00:36

von VINCENT WIDDIG

Cyberspiona

und Cyberkriegsführung stehen im Mittelpunkt der aktuellen Debatten. Vor allem, da immer mehr Staaten diese neuen Mittel als eine legitime und notwendige Erweiterung ihrer militärischen Fähigkeiten betrachten. Jetzt rüstet auch die Bundeswehr auf – virtuell. Bundesministerin der Verteidigung Ursula von der Leyen hat kürzlich die Schaffung einer neuen Abteilung „Cyber- und Informationsraum“ (CIR) angekündigt. Mit ihr soll die Bundeswehr von nun an in der Lage sein, auch auf dieser Ebene gegen mögliche Bedrohungen vorzugehen. Allerdings stellte die Ministerin bereits bei der Ankündigung der Abteilung CIR ihre defensive Rolle klar: „Offensiv wäre […] hinter die Firewall eines möglichen Gegners [zu gehen], das dürfen und wollen wir nicht“. Ebenso im Vorfeld ausgeschlossen wurde das Ausspähen militärischer Daten fremder Nationen.

Auch wenn der Bedarf an einer reinen defensiven Abteilung nicht von der Hand zu weisen ist; bleibt schon vor dem Hintergrund der Pegasus- (Urteil v. 23. September 2015 – 2 BvE 6/11 – Rn. 1-125) und AWACS-II-Rechtsprechung (BVerfGE 121, 135 – 175) des BVerfG die Frage nach einem möglichen parlamentarischen Ermächtigungsvorbehalt für eventuelle Offensivaktionen der CIR offen. Ebenso wie die Einordnung der „Spionage“ durch das BMVg. Um so überraschender ist es, dass die vielfach vollzogene exzessive Auslegung von (Cyber-)Offensivaktionen als bewaffneter Angriff unter dem völkerrechtlichen *ius ad bellum* auf Wehrverfassungsebene scheinbar so übernommen wurde, dass die Bundeswehr außerhalb der Defensivmaßnahmen nur mit Bundestagsmandat tätig werden darf.

Fallen offensive (Cyber-)Maßnahmen überhaupt unter das völkerrechtliche Gewaltverbot?

Trotz der anfänglichen Mystifizierung des Cyberspace als „fünfte Dimension“ in Analogie zu bekannten Räumen wie der See oder dem Weltraum und der mit ihnen verbundenen Referenz der Güter als *res communis omnium* sind die meisten Staaten mittlerweile darüber übereingekommen, dass die geltenden völkerrechtlichen Regeln auf den Cyberraum grundsätzlich anwendbar sind. Ein erster fruchtbarer Ansatz in dieser Entwicklung stellt insoweit das von einer internationalen Expertenkommission erarbeite Tallinn Manual on the International Law applicable to Cyber Warfare dar. Die hierbei erarbeiten Regeln zum *ius ad bellum und ius in bello* haben die bisherige Praxis merkbar beeinflusst.

Leitet man aus der völkerrechtlichen Einordung solcher Aktionen eine wehrverfassungsrechtliche Folge ab (schon vor dem Hintergrund des Artikels 26 GG), scheint die grundsätzliche Forderung nach einer parlamentarischen Ermächtigung aller (Cyber-)Offensivmaßnahmen fragwürdig. Konkret geht es im *ius ad bellum* um die Einstufung einer (Cyber-)Offensivmaßnahme als bewaffneter Angriff und damit als verbotene Gewaltanwendung nach Artikel 2 Absatz 4 UN-Charta. Die Folge kann die Auslösung des in Artikel 51 UN-Charta kodifizierten naturgegebenen Selbstverteidigungsrechts sein. Ungeachtet der Frage, ob eine (Cyber-)Offensivmaßnahme als Anwendung von Gewalt und im Sinne von Artikel 2 (4) UN-Charta zu klassifizieren ist, stellt nicht gleich jede Gewaltanwendung einen bewaffneten Angriff dar. Zur Auslösung des individuellen bzw. kollektiven Selbstverteidigungsrechts muss die Gewaltanwendung die Schwelle eines gewissen Ausmaßes und Wirkung (scale and effects) überschreiten. Weitestgehende Einigkeit besteht mittlerweile darüber, dass Daten keine Objekte darstellen und somit Operationen, die allein auf den Cyberraum beschränkt sind, grundsätzlich keine Gewaltanwendung darstellen können. Zu denken wäre in einigen Fällen lediglich an einen Verstoß gegen das Interventionsverbot oder das Verbot zwischenstaatlicher Schädigungen. Ein Schluss, zu dem auch die internationale Expertenkommission in Regel 11, para 3 des Tallinn Manuals kommt. Das vielfach angebrachte Szenario des Angriffs auf die New Yorker Börse geht hier ebenfalls fehl. Trotz der wohl erheblichen Schäden für die US-amerikanische Volkswirtschaft stellen rein wirtschaftliche Schäden keine Anwendung von Gewalt dar. Eine Ausnahme soll lediglich bei Angriffen auf sog. kritische Infrastruktur bestehen, soweit sie eine gewisse Wirkung entfalten. Diese rein auf die Wirkung fokussierte Ansicht verkennt zwar, dass nicht die reine Anwendung von Gewalt – unabhängig von eventuellen Schäden – sondern nur die Anwendung *militärischer* Gewalt ein Verstoß gegen Artikel 2 (4) UN-Charta und für die Auslösung des Selbstverteidigungsrechts, welches eine kinetische Reaktion rechtfertigen würde, ursächlich sein kann. Der in Artikel 51 UN-Charta geforderte „bewaffnete Angriff“ (agression armée) setzt hier jedenfalls die Anwendung von Mitteln und Methoden der Kriegsführung voraus, die ihrem Ausmaß und Wirkung nach einem konventionellen Angriff gleichkommen. Wie sich in der Staatenpraxis gezeigt hat, erfolgt ein Ausschluss von nicht-staatlichen Akteuren hierdurch nicht zwangsläufig (vgl. Regel 13, para 17 Tallinn Manual). Allerdings ist nicht auszuschließen, dass die Staaten hier aufgrund ihrer Verwundbarkeit auch dann gewillt sein werden eine Gewaltanwendung

anzunehmen, selbst wenn der Angriff als solcher keine Schäden außerhalb des Cyberspace verursacht hat.

Ein Großteil der Cyber-Maßnahmen der Abteilung CIR wird wohl der „Erkenntnisgewinnung“ zuzuordnen sein. Sollte es sich hier um (Cyber-)Spionage handeln, stellt sich die Frage nach ihrer Zulässigkeit und ob sie nicht auch als Grund für einen bewaffneten Konflikt zu werten ist. Zwar kennt das Völkerrecht keine explizite Erlaubnis für Spionage, die Staaten verbieten allerdings im nationalen Strafrecht Spionage gegen sich selbst. Geht man nun vom *Lotus-Prinzip* aus, wird man jedoch auch kein generelles Verbot der Spionage feststellen können. Wie auch immer man (Cyber-)Spionage einzuordnen vermag, letztlich wird auch sie nicht die Schwelle eines bewaffneten Angriffes erreichen, da Ausmaß und Folgen dieser Maßnahmen so gut wie nie jene eines konventionellen Angriffes erreichen werden. Ob sie darüber hinaus *per se* einen Verstoß gegen das Interventionsverbot darstellt, stellt nicht nur die internationale Expertenkommission (Regel 10, para 10 Tallinn Manual) in Frage, da hier in der Regel das Zwangselement (zu einem Handeln oder Unterlassen) fehlen wird.

In jedem Fall werden diese Maßnahmen wohl nicht als Gewaltanwendung zu klassifizieren sein. Ob daher das Gros der (Cyber-)Offensivmaßnahmen überhaupt die Schwelle zur Gewaltanwendung überschreiten können, ist mehr als zweifelhaft.

Impliziert die völkerrechtliche Auslegung auch die Rechtmäßigkeit auf Verfassungsebene?

Auf wehrverfassungsrechtlicher Ebene steht und fällt die Sache spätestens mit einem Parlamentsvorbehalt auslösenden „Einsatz bewaffneter Streitkräfte“. Das BVerfG hat sich insoweit in seiner AWACS-II Entscheidung hierzu geäußert und stellte fest:

> „Ein unter dem Grundgesetz nur auf der Grundlage einer konstitutiven Zustimmung des Deutschen Bundestags zulässiger Einsatz bewaffneter Streitkräfte liegt vor, wenn deutsche Soldaten in bewaffnete Unternehmungen einbezogen sind“ (BVerfGE 121, 163).

Liegt also die Einbeziehung deutscher Streitkräfte in bewaffnete Unternehmungen vor, ist dies immer auch ein Einsatz bewaffneter Streitkräfte, der – unabhängig von der tatsächlichen Bewaffnung – der Zustimmung des Parlaments bedarf. Konkretisiert (und bestätigt in der Pegasus-Entscheidung) wurde dies durch das BVerfG dahingehend, dass relevant für die Zustimmungsbedürftigkeit die Erwartung einer konkreten Einbeziehung ist. Für diese qualifizierte Erwartung bedarf es:

> „[…] hinreichend greifbarer tatsächlicher Anhaltspunkte dafür, dass ein Einsatz […] in die Anwendung bewaffneter Gewalt münden kann“, sowie
>
> „[…] einer besonderen Nähe der Anwendung von Waffengewalt [, deren Einbeziehung] unmittelbar zu erwarten [ist]. Steht die Anwendung von Waffengewalt zeitlich nahe bevor, begründet dies bereits für sich genommen die qualifizierte Erwartung […]“(BVerfGE 121, 165-66).

Die o.g. Definition versuchte auch schon die Bundesregierung im Rahmen der Operation „Pegasus“ für sich zu nutzen und wertete die Aktion nicht als „Einsatz bewaffneter Streitkräfte“. Dem schob das BVerfG zwar teilweise einen Riegel mit der Betonung des wehrverfassungsrechtlichen Parlamentsvorbehalts als wirksames Mitentscheidungsrecht des Bundestages vor. Soweit dem Grundgesetz eine Zuständigkeit des Deutschen Bundestages mittels eines Mitentscheidungsrechts entnommen werden könne, entfiele ein eigenverantwortlicher Entscheidungsspielraum der Bundesregierung. Selbst wenn man jedoch von diesem im Pegasus-Urteil des BVerfG bestätigten Grundsatz ausgeht, kommt man bei den meisten Cyber-Angriffen kaum weiter.

Fällt der Cyber-Angriff also aus dem Anwendungsbereich von Artikel 87a GG?

Die meisten Offensivmaßnahmen werden schon mangels Einstufung als bewaffneter Angriff kaum eine realistische Einbeziehung in bewaffnete Auseinandersetzungen zur Folge haben und somit aus dem Anwendungsbereich des Artikels 87a GG fallen. Dies ist in der Regel auch dann anzunehmen, stellt man allein auf die Erheblichkeit der Handlung des eingesetzten Soldaten für den (auch im internationalen Verbund stattfindenden) betreffenden Einsatz ab. Auch sonst erscheint die Subsumtion der meisten Cyberaktionen der CIR unter die o.g. Voraussetzungen nicht wahrscheinlich. Der die Parlamentsbeteiligung auslösende „Einsatz bewaffneter Streitkräfte“ liegt schlicht mangels der notwendigen erheblichen physischen Wirkung oder Handlung nicht vor. Ausnahmen können lediglich Angriffe auf kritische Infrastrukturen sowie solche, die nach Ausmaß und Wirkung einem konventionellen Angriff gleichen, sein. Liegt eine ausreichende „scale and effects“-Wirkung der Maßnahme vor, ist an eine konstitutive Beteiligung des Parlaments zu denken. In jedem Fall werden (auch) offensive Cyber-Maßnahmen so gut wie immer bereits beendet sein, bevor das Parlament überhaupt befragt werden kann. Der praktische (rechtliche) Nutzen einer nachgelagerten parlamentarischen Kontrolle scheint indes höchst fragwürdig, da selbst bei Nichtbilligung der Aktion ihre praktischen Folgen unumkehrbar sein werden. Dies erkennt auch richtigerweise das BVerfG im Pegasus-Urteil, in dem es konstatiert:

> „Wenn ein rechtserheblicher parlamentarischer Einfluss auf den konkreten Einsatz der Streitkräfte aus tatsächlichen Gründen nicht mehr möglich ist, ergibt sich aus dem wehrverfassungsrechtlichen Parlamentsvorbehalt keine Pflicht der Bundesregierung, eine Beschlussfassung des Bundestages herbeizuführen“.

Die Bundesregierung trifft hier lediglich eine unverzügliche und qualifizierte Unterrichtungspflicht gegenüber dem Deutschen Bundestag. Eine effektive parlamentarische Kontrolle wird somit fast unmöglich gemacht.
